DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

DEC 7 1998

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR OF ADMINISTRATION AND MANAGEMENT
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Web Site Administration

This memorandum provides the DoD policy, assigns responsibility, and describes the procedures for establishing, operating and maintaining DoD unclassified Web sites. DoD is committed to maximizing the availability of timely and accurate Defense information to the public as well as maintaining a secure framework for our use of Internet-based technologies. At the same time, we must be continually mindful of our responsibility to protect our most precious resource–our men and women who serve this Nation, and their families.

To accomplish the above, all DoD Components have the responsibility to ensure sound information assurance practices are in place and operating for Web sites. Heads of Components shall be responsible for managing the use and content of the information placed on the Web consistent with the guidance and processes contained in the attached. This memorandum cancels the joint ASD (PA) and ASD (C3I) memorandum entitled "Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service," and dated July 18, 1997 (as amended).

In view of the changing environment and the impact of information technology on the sensitivity of information, I further direct that within the next 120 days:

- The DoD General Counsel lead a review of statutes as they relate to our ability to safeguard sensitive, unclassified information and advise me of any recommended changes;

- The Director Administration and Management lead a review of "privacy-related" policies, and release of information to ensure that we are maintaining the proper balance with respect to individuals' privacy;

- The USD (A&T) lead a review of the Department's ability to safeguard sensitive, unclassified information in our electronic commerce systems.

I further direct that the Senior Civilian Official OASD(C3I), working with the ASD (PA) and the Director of Administration and Management ensure that the web site administration policy and procedures are codified in the DoD Publication System within 120 days.

Comments, suggestions and recommendations for changes to the attached policy and guidance should be directed to OASD(C3I). An electronic copy of this guidance is available at http://www.defenselink.mil/admin/about.html#WebPolicies.

John J. Hamre

Attachment

Web Site Administration

Policies & Procedures

November 25, 1998

With Amendment April 26, 2001 incorporated in red italics

Office of the Assistant Secretary of Defense
(Command, Control, Communications & Intelligence)
6000 Defense Pentagon
Washington, DC 20301-6000

Department of Defense
WEB SITE ADMINISTRATION
GUIDANCE

CONTENTS

DEPSECDEF Memorandum Subject: Web Site Information Services DoD-Wide, dated November 25, 1998 implements the policies, responsibilities and procedures for Web Site Administration. An electronic copy of this guidance is available at http://www.defenselink.mil/admin/about.html#WebPolicies. Please forward comments, suggestions and recommendations for changes to: OASD (C3I), ODASD (Policy & Implementation/Deputy CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

WEB SITE ADMINISTRATION

Part I – Policy & Responsibilities

November 25, 1998

1. PURPOSE

This document delineates the policy and assigns responsibility related to establishing, operating and maintaining unclassified Web sites and other related services. It supersedes the "Guidelines for Establishing and Maintaining a Publicly Accessible Department of Defense Web Information Service" jointly published by the Office of the Assistant Secretary of Defense (Public Affairs) and the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on July 18, 1997 (updated January 9, 1998).

2. APPLICABILITY

This policy applies to:

2.1. The Office of the Secretary of Defense (OSD), the Military Departments (including the Coast Guard when it is operated as a Military Service in the Navy), the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Defense Agencies, and the Department of Defense (DoD) Field Activities (hereafter referred to collectively as "the DoD Components") and to their contractors and consultants including those who operate or maintain DoD Web sites for them, through incorporation into contracts.

2.2. All unclassified DoD Web sites, both publicly and non-publicly accessible.

2.3. Reviewing approval requests received from DoD contractors and subcontractors relative to the posting of unclassified DoD information to a DoD contractor Web site.

3. DEFINITIONS

Terms used in this document are defined in Part III.

4. POLICY

It is the policy of the DoD that:

4.1. Using the World Wide Web is strongly encouraged in that it provides the DoD with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies and programs.

4.2. The considerable mission benefits gained by using the Web must be carefully balanced through the application of comprehensive risk management procedures against the potential risk to DoD interests, such as national security, the conduct of federal programs, the safety and security of personnel or assets, or individual privacy created by having electronically aggregated DoD information more readily accessible to a worldwide audience.

4.3. Each organization operating a DoD Web site will implement technical security best practices with regard to its establishment, maintenance and administration.

4.3.1. DoD Web sites containing i) FOR OFFICIAL USE ONLY information, ii) information not specifically cleared and marked as approved for public release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)), or iii) information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the DoD, especially in electronically aggregated form, must employ additional security and access controls. Web sites containing information in these categories should not be accessible to the general public.

4.4. Consistent with other leadership responsibilities for public and internal communication, the decision whether or not to establish an organizational Web site, and to publish appropriate instructions and regulations for a Web site within the limitations established by this document, is hereby delegated to each DoD Component.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I)) shall:

5.1.1. Provide policy and procedural guidance with respect to establishing, operating and maintaining Web sites.

5.1.2. Maintain liaison with the Assistant Secretary of Defense for Public Affairs to provide policy oversight and guidance to ensure the effective dissemination of defense information via the Internet.

5.1.3. Provide technical support consistent with existing Chief Information Officer (CIO) responsibilities.

5.1.4. Develop and maintain, in coordination with the Chairman of the Joint Chiefs of Staff, Under Secretary of Defense (Personnel &Readiness), and General Counsel, training guidance and requirements that addresses information security on the Web.

5.1.5. Approve and publish DoD Instructions and Publications, as necessary, to guide,direct, or help Web site activities, consistent with DoD 5025.1-M (reference (kk)).

5.1.6. Provide a mechanism for feedback reporting across DoD, to include "Lessons Learned" and the identification of useful automated tools to aid in the conduct of multi-disciplinary security assessments of Web sites.

5.1.7. Ensure compliance with this policy.

5.2. The Assistant Secretary of Defense for Public Affairs (OASD (PA)) shall:

5.2.1. Operate and maintain DefenseLINK (http://www.defenselink.mil) as the official primary point of access to DoD information on the Internet.

5.2.2. In coordination with the other OSD Principal Staff Assistants, provide oversight policy and guidance to ensure the absolute credibility of defense information released to the public through publicly accessible Web sites.

5.2.3. Establish and maintain a central Web site registration system for the Department that meets the requirements for the Government Information Locator Service (GILS) and is integrated with Service-level registration systems.

5.3. The Assistant Secretary of Defense for Reserve Affairs and the Chairman of the Joint Chiefs of Staff shall develop and implement a plan that uses Reserve Component assets to conduct ongoing operations security and threat assessments of Component Web sites.

5.4. The Secretaries of the Military Departments shall establish and maintain a central registration system for the respective service that meets the requirements for GILS and is integrated with DefenseLINK.

5.5. The Heads of the DoD Components shall:

5.5.1. Establish a process for the identification of information appropriate for posting to Web sites and ensure it is consistently applied.

5.5.2. Ensure all information placed on publicly accessible Web sites is properly reviewed for security, levels of sensitivity and other concerns before it is released. Detailed requirements for clearance of information for public release are located in DoD Directive 5230.9 and DOD Instruction 5230.29 (references (h) and (o)) and Part II of this document.

5.5.3. Ensure approved DoD security and privacy notices and applicable disclaimers are used on all Web sites under their purview.

5.5.4. Ensure all information placed on publicly accessible Web sites is appropriate for worldwide dissemination and does not place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

5.5.5. Ensure procedures are established for management oversight and regular functional review of the Web site.

5.5.6. Ensure operational integrity and security of the computer and network supporting the Web site is maintained.

5.5.7. Ensure that reasonable efforts are made to verify the accuracy, consistency, appropriateness, and timeliness of all information placed on the Web site.

5.5.8. Register each publicly accessible Web site with the Government Information Locator Service (GILS).

5.5.9. Provide the necessary resources to adequately support Web site operations to include funding, equipping, staffing and training.

5.5.10. Ensure that a comprehensive, multi-disciplinary security assessment is conducted of their Web sites within 120 days of the promulgation of this document, and at least annually thereafter.

5.5.11. Provide a mechanism for feedback reporting within the Component, to include “Lessons Learned” suitable for all DoD Components.

5.5.12. Ensure compliance with this policy for those functions, missions, agencies, and activities in their purview.

5.5.13. Grant waivers on a non-delegable basis to a provision of the procedures contained in Part II of this document when it has been determined that immediate implementation would adversely impact essential mission accomplishment. Instances where such waivers have been granted will be reported to the Assistant Secretary of Defense (C3I).

6. EFFECTIVE DATE. This policy is effective immediately.

WEB SITE ADMINISTRATION

Part II – Procedures

November 25, 1998

With Amendment April 26, 2001 incorporated in red italics

1. PURPOSE

This document delineates the processes and procedures related to establishing, operating and maintaining unclassified Web sites and other related services. It also provides guidelines for the review of material prior to its posting to Web sites.

2. WEB SITE ESTABLISHMENT

2.1. Support of Mission. Each Web site shall have a clearly defined purpose that supports the mission of the DoD Component. The Head of the DoD Component, or his/her designee in accordance with official policies, shall approve the defined purpose and general content of the Web site. Non-copyrighted material, text, clip art, hypertext links, images and sound or video clips may be used only if they directly relate to the Component's mission.

2.2. Web Site Security Accreditation. Each organization establishing a Web site shall institute a security certification and accreditation procedure in accordance with DoD Directive 5200.40 (Reference (v)). Successful implementation depends on defining security requirements early in the process of establishing a Web site. All security-related disciplines (computer, communications, personnel, etc.) shall be considered in the requirements definition for the Web site. Cost versus risk tradeoffs shall be evaluated and security requirements assigned accordingly.

2.3 Single Source Information. For the purpose of preventing duplication on the Web, a Web site shall normally be limited only to information for which the establishing organization is responsible. Web sites that contain information pursuant to the requirements of the Electronic Freedom of Information Act, 5 USC 552(a)(2)(D) & (E) (reference (j)) are exempt from this restriction. Information from other sources on the Internet will not be copied but will be referenced or otherwise linked. This does not prevent information providers from mirroring or replicating information for performance, security or other mission-related reasons. However, when this is done, the information provider posting the replicated file on its server should contact the content owner of the information and obtain written permission to replicate the information. No copyrighted information may be posted in this process without the permission of the copyright owner. Procedures must also be established for updating the information. In addition, the releasability of the information must be verified by the source from which it is copied. The DoD information provider should continue to control the information to ensure its protection from inappropriate manipulation and make reasonable efforts to verify its currency and accuracy.

2.4. Web Site Registration. All DoD Web sites shall register with the appropriate Service-level site or directly with DefenseLINK.

3. INFORMATION POSTING PROCESS

3.1. DoD Component Heads and Heads of subordinate organizations that establish Web sites are responsible for instituting a process for the identification of information appropriate for posting to Web sites and the appropriate security and access controls. The steps of this process (see illustration 1) include:

3.1.1. Identification of information that needs to be conveyed quickly and efficiently and thus will benefit from the attributes of the Web;

3.1.2. Identification of a specific target audience for the information;

3.1.3. Identification of the DoD Originating Office for the information if the sensitivity of the information or distribution restrictions on its release cannot be readily ascertained;

3.1.4. Review of the content for sensitivity and distribution/release controls, including sensitivity of information in the aggregate;

3.1.5. Determination of the appropriate access and security controls;

3.1.6. Approval of the information for public release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)) if it is to be posted to a publicly accessible Web site;

3.1.7. Posting the information, once all required steps have been taken;

3.1.8. Verification; and

3.1.9. Feedback reporting, to include “Lessons Learned.”

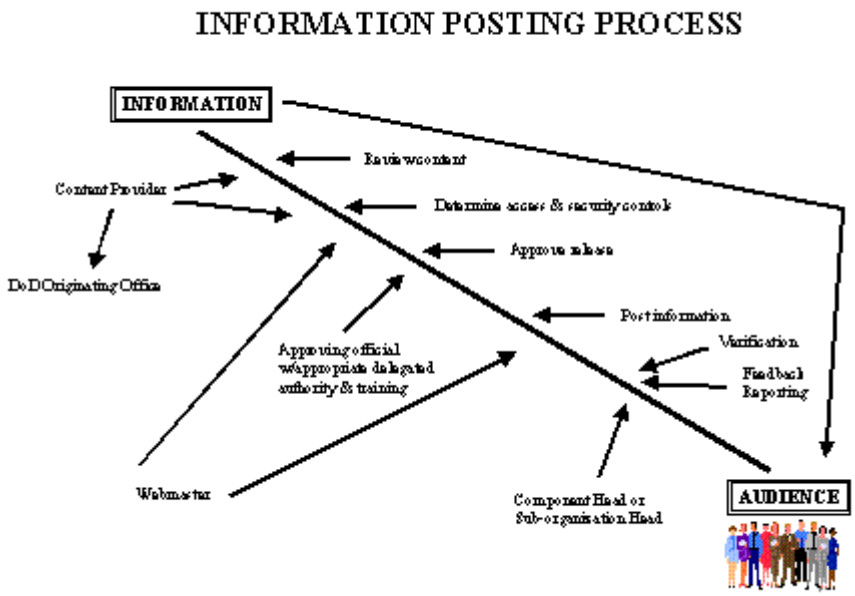

Illustration 1. Information Posting Process

3.2 Identification of Information. The World Wide Web provides the DoD with a powerful tool to convey suitable information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies and programs. It is at the heart of the Defense Reform Initiative and is key to the reengineering and streamlining of our business practices. The American democratic process rests on the right of our citizens to know what government is doing, and the corresponding ability to judge its performance. Access to information by the public through the Web is an important component of this right. Nevertheless, careful examination of the potential consequences of placing information on the Web must be undertaken before it is made available.

3.2.1. The identification of a need to post information to a Web site will normally be made by the entity that generates the information and thus has the best knowledge of its content.

3.3. Identification of Target Audience. Illustration 2 depicts many of the target audiences for DoD information posted to the Web. Only information of value to the general public and which does not require additional protection should be posted to publicly accessible sites on the World Wide Web. Information requiring additional protection, such as FOR OFFICIAL USE ONLY (FOUO) information, information not specifically cleared and approved for public release, or information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the DoD, including military personnel and civilian employees, should be placed on Web sites with security and access controls.

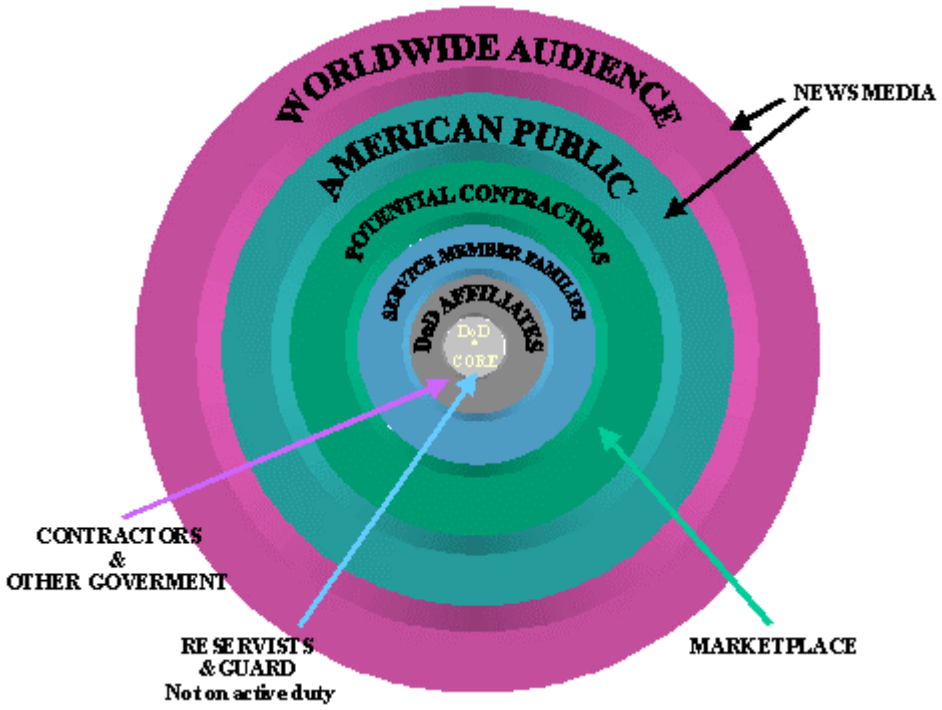

Illustration 2. Target Audience

3.4. DoD Originating Office (DOO). Is the entity that created or sponsored the work that generated the information or received/acquired the information on behalf of the DoD. The DOO has the responsibility for assigning appropriate markings to information to include its sensitivity (i.e. classified, FOR OFFICIAL USE ONLY, or other distribution control markings for unclassified information), its releasability to the public, and the approved audience for access (e.g. DoD only, contractors, general public, etc.). The DOO shall be consulted whenever there is doubt with regard to the sensitivity of the information or distribution restrictions on its release.

3.5. Content Review.

3.5.1. Clearance Requirements for Publicly Accessible Web Sites. Heads of DoD Components must establish, in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)), clearance review procedures for official DoD information that is prepared by or for DoD personnel and is proposed for posting to publicly accessible Web sites.

3.5.2. The above procedures must address the need for trained and knowledgeable personnel, familiar with the rules governing FOR OFFICIAL USE ONLY (FOUO) information as well as pertinent security classification guides, as appropriate. Such individuals must also be familiar with the aspects of the organization's operations considered critical, its vulnerabilities, as well as the pertinent threat in order to assess the nature of the risk associated with posting specific information to Web sites. This risk assessment must also include the increased sensitivity of certain information when electronically aggregated in significant volume.

3.5.2.1. In assessing the increased sensitivity that information may assume in electronic format, it is necessary to take into account the attributes of data mining (i.e., the nontrivial extraction of implicit, previously unknown, and potentially useful information from data). Data mining uses machine learning, statistical and visualization techniques to discover and present knowledge in a form, which is easily comprehensible to humans.

3.5.2.2. The content provider will also take into account the form in which the information was distributed, such as press releases, press conferences, or publicly disseminated documents, the susceptibility of the information to data mining, and the likelihood that the information could directly lead to the discovery and presentment of knowledge that is otherwise controlled (e.g., classified information or FOUO information). Also to be assessed is a specific risk to the Department's credibility if publicly released information is omitted and/or deleted from the Web.

3.5.2.3. If the overall risk resulting from posting the information is determined to be unacceptable, the information must be afforded security and access controls. Part V of this document provides additional guidance in this area while the paragraphs below provide specific prohibitions.

3.5.3. FOR OFFICIAL USE ONLY (FOUO). Information, the disclosure of which would cause a foreseeable harm to an interest protected by one or more of the exemptions to the Freedom of Information Act (FOIA), shall not be posted to a publicly accessible Web site. This information is designated FOUO pursuant to reference (j). While records containing FOUO information will normally be marked at the time of their creation, records that do not bear such markings shall not be assumed to contain no FOUO information without examination for the presence of information that requires continued protection and qualifies as exempt from public release. This may require coordination with the DOO for the information. The following examples are illustrative of the type of information that may be considered to be FOUO. **These examples are not an exclusive listing and they are not intended to offer any guidance in responding to Freedom of Information Act (FOIA) requests.**

3.5.3.1. Analysis and recommendations concerning lessons learned which would reveal sensitive military operations, exercises or vulnerabilities.

3.5.3.2. Reference to unclassified information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of a military plan or program.

3.5.3.3. Personal information including compilations of names of personnel assigned to overseas, sensitive, or routinely deployable units.

3.5.3.4. Information, the release of which would be a clearly unwarranted invasion of personal privacy, to include the following categories about U.S. citizens, DoD employees and military personnel: 1) Social Security Account Numbers; 2) dates of birth; 3) home addresses, and 4) telephone numbers other than duty office numbers. Duty phone numbers

of units described in paragraphs C.3.2.1.6.2.2. of DoD 5400.7-R (reference (j)) may not be posted.

3.5.3.5. Names, locations, and specific identifying information about family members of DoD employees and military personnel.

3.5.3.6. Proprietary information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial and financial information submitted by an entity outside the government which considers the information to be protected from release to the public.

3.5.3.7. Test and evaluation information that could result in an unfair advantage or disadvantage to the manufacturer or producer.

3.5.3.8. Technical Information not marked or otherwise determined to be appropriate for Distribution Statement A in accordance with DoD Directive 5230.24 (reference (r)). This includes all technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment.

3.5.4. Unclassified information pertaining to classified programs. The clearance review procedures for unclassified information pertaining to classified programs proposed for posting to a publicly accessible Web sites must take into account the likelihood of classification by compilation. Consultation with the program security classification guide may be required to determine the likelihood that the information, if compiled or aggregated with other information likely to be contained on publicly accessible Web sites, will reveal an additional association or relationship that meets the standards for classification under DoD 5200.1-R (reference (kk)). If such information is posted to a Web site, it must be afforded security and access controls as specified in Part V of this document.

3.5.4.1. In instances where a question arises as to whether information in compilation/aggregation requires protection as classified information, and the information has not yet been entered onto the Web site, the DOO(s) for the information shall be contacted to obtain a decision on the matter before the information is posted. Where the information has already been posted, the information will be withdrawn from the system and will not be re-posted until a decision is obtained from the DOO(s) for the information. In instances where there is a conflict among the DOOs as to the sensitivity of the information, which they are unable to resolve, the matter may be referred to the next higher level within each of the DOOs' organizations until a resolution can be obtained.

3.5.4.2. Users of a Web site who believe that information in compilation or aggregation on a system or systems to which they have access contains classified information, should contact the webmaster of the system(s) in question or, if the webmaster is unknown, report the matter to their own organization's security office for evaluation and action as appropriate.

3.5.4.3. When conducting multi-disciplinary security assessments of Web sites, advanced search engines (e.g. high-end natural-language-based systems optimized for English syntax analysis) and other automated means will be used to assess the likelihood of the presence of information classified by compilation

3.5.5. Copyrighted Material. Copyrighted material will be used only when allowed by prevailing copyright laws and may be used only if the materials relate to the Component's mission. Consult with Counsel when using any copyrighted material.

3.5.6. Conflicts of Interest. In accordance with the Joint Ethics Regulation (reference (k)), product endorsements or preferential treatment of any private organization or individual shall not appear on any official DoD publicly accessible site.

3.6. Access Controls.

3.6.1. A DoD Web site may not post FOR OFFICIAL USE ONLY information, or information not specifically cleared and approved for public release unless it employs adequate security and access controls. Information of questionable value to the general public must be evaluated before worldwide dissemination to assess the risk to the DoD. Adequate security and access controls must likewise be employed for such information if it is determined to place national security, DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

3.6.2 Determinations as to the appropriate security and access controls to employ will be based upon the sensitivity of the information, the target audience for which the information is intended, and the level of risks to DoD interests. Part V of this document contains additional guidance.

3.6.3. Publicly accessible DoD Web sites will not normally contain links or references to DoD Web sites with security and access controls. Under certain circumstances, however, it may be appropriate to establish a link to a log-on site provided details as to the controlled site's contents are not revealed.

3.7. Release Approval. Approvals for posting of information to publicly accessible Web sites must be in accordance with the provisions of DoD Instruction 5230.29 (reference (o)). Approvals can be granted only by an appropriately trained individual specifically delegated that authority by the Head of the DoD Component or his or her designee.

3.8. Information Posting. Once the procedures established in paragraphs 3.2, 3.3, 3.5, and 3.6. have been completed, the information may be posted to the Web. In addition, the following steps must be accomplished:

3.8.1. A reasonable effort to validate the accuracy of the information.

3.8.2. All links associated with the Web site have been validated.

4. ADMINISTRATION AND VERIFICATION

4.1. Web Server Environment Administration. Procedures governing the administration of the Web server environment must be established and, as a minimum, address the following:

4.1.1. Operation of the Web server environment.

4.1.2. Security of the Web server environment.

4.1.3. Maintenance of access and security control features and ensuring that warning and consent to monitoring notices are posted as appropriate.

4.1.4. Ensuring designated approving authority (DAA) approval is re-accomplished if any configuration changes are made to the Web server environment.

4.1.5. Ensuring all links from pages under its control are appropriate and valid.

4.1.6. Establishing procedures for content providers and page maintainers to place information on the Web server.

4.1.7. Granting and monitoring write-access privileges.

4.1.8. Maintaining and evaluating audit control logs.

4.1.9. Gathering and analyzing performance data.

4.1.10. Developing, coordinating, publishing, maintaining, and testing support plans for contingency and service restoration.

4.1.11. Coordinating mirror or replication sites with other system administrators, as required.

4.1.12. Implementing security and access controls requested by content providers and page maintainers as required.

4.1.13. Ensuring access lists are maintained where appropriate.

4.1.14. Incorporating a feedback mechanism for users' comments in accordance with the Paperwork reduction Act of 1995 (reference (a)).

4.2. Verification. Procedures must be established for each DoD Web site to ensure that:

4.2.1. A comprehensive, multi-disciplinary security assessment addressing both content and technical issues is conducted at least annually.

4.2.2. Periodic reviews are conducted to assess compliance with established information posting procedures.

4.2.3. Outdated or superseded information is identified and promptly removed from the system or appropriately archived.

4.3. Feedback Reporting.

4.3.1. Reserve component assets used for DoD-wide OPSEC and threat assessment of unclassified DoD Web sites will observe feedback reporting to include “Lessons Learned.”

4.3.2. Web site content providers and administrators will support and participate in the feedback reporting system.

4.3.3. Web site content providers and administrators will review “Lessons Learned” and incorporate content and security changes where appropriate.

5. System Security Considerations

5.1. Operators of DoD Web server environments shall be trained in technical information security best practices, or shall have immediate access to appropriately trained individuals. Security maintenance and administration shall be considered an essential element of Web site operation and maintenance at all times.

5.2. A formal risk assessment shall be conducted at each organization operating a DoD Web site to determine the appropriate risk management approach based on the value of the information; the threat to the DoD Web server environment and the information contained thereon; the vulnerability of the DoD Web server environment and the information contained thereon; and the countermeasures employed by the DoD Web server environment. A security policy shall be written for each DoD Web server environment or multiple sites furnishing similar data on the same system infrastructure or architecture based on the results of the risk assessment.

5.3. DoD Web servers that are externally accessed shall be isolated from the internal network of the sponsoring organization. The isolation may be physical, or it may be implemented by technical means such as an approved firewall. The server software will be FIPS 140-1 compliant with all security patches properly installed. Approved DoD security protocols will be used for all Web servers. Additional security measures shall also be employed consistent with

the risk management approach and security policy of the individual DoD Web site. Examples of additional measures to be considered include:

5.3.1. Disable IP forwarding, avoid dual-homed servers

5.3.2. Employ least privilege

5.3.3. Limit functionality of Web server implementation

5.3.4. Employ tools to check configuration of host

5.3.5. Enable and regularly examine event logs

5.4. In addition, all DoD Web servers shall employ a back-up methodology as part of the Web site architecture. Information shall be replicated to the back-up environment to ensure that the information will not be lost in the event that the Web server environment is corrupted, damaged, destroyed or otherwise compromised.

5.5. In cases where an organization operating a DoD Web site determines a requirement to host both a public and non-public Web server, then additional security measures shall be required for the non-public Web server. At minimum, appropriate access controls, audit of security events, and additional measures to ensure confidentiality, integrity and availability of the information shall be employed (see Part V).

5.6. ID and Password Protection. The Internet is an unsecured network where compromise of user ID and password can occur during open transmission. IDs and passwords should not be transmitted without encryption. Secure protocols (e.g. secure sockets layer (SSL) protocol) provides a transmission level of encryption between the client and server machines.

5.7. It is essential that DoD Web server environment be implemented and maintained by certified personnel in accordance with OSD memorandum, subject: Information Assurance (IA) Training and Certification (reference (ll)). Day-to-day maintenance of the hardware and software, including security patches and configurations, is essential to the system security posture of DoD Web server environments.

6. GOVERNMENT INFORMATION LOCATOR SERVICE (GILS) REQUIREMENT

DefenseLINK is the central registration point for DoD Web sites. Each Service-level site will establish and maintain registration systems, integrated with DefenseLINK, for their Service. All DoD Web sites shall register with the appropriate Service-level site or directly with DefenseLINK. As part of the registration process, a release authority for the information must be named and the entrant must certify that the content of the Web site complies with the policies set forth in the issuance.

7. PRIVACY AND SECURITY NOTICE

A privacy and security notice must be given to users of each Web site and shall be prominently displayed or announced on at least the first page of all major sections of each Web site. . *The notice describes how, in general, security is maintained on the site, and what specific information is collected, why it is collected, and how it is used. All information collected must be described in this notice.* Providing a statement such as "Please read this privacy and security notice." linked to the actual notice is satisfactory. Organizations shall avoid flashy graphics or other indicators that create a misperception of danger, such as skull-and-crossbones logos or "warning" signs. *Agencies subject to DoD Directive 5240.1 (reference (q)) must comply with its provisions. See paragraph 12 below for details and limitations regarding the collection of information, including information voluntarily provided by the user (e.g., e-mail to the webmaster). See Part V for the text of the required privacy and security notice.*

8. EXTERNAL LINKS

8.1. Approval. The ability to hyperlink to sources external to your organization is a fundamental part of the World Wide Web, and can add significant value to the functionality of publicly accessible DoD Web sites. DoD Components must establish objective and supportable criteria or guidelines for the selection and maintenance of links to external Web pages.

8.1.1. Links to non-DoD Web resources should support the organization's mission. External links should be reviewed periodically to ensure their continued suitability. If the content of a linked external site becomes questionable or objectionable, remove the link.

8.1.2. In accordance with DoD 5500.7-R (reference (k)), no product endorsements or preferential treatment shall be given on publicly accessible official DoD Web sites.

8.1.3. No payment of any kind shall be accepted in exchange for a link placed on an organization's publicly accessible official DoD Web site.

8.1.4. In accordance with DoD 5500.7-R, publicly accessible DoD Web sites shall not require or encourage users to choose any specific browser software. Only text or hyperlinked text shall be used to direct visitors to software download sites. Graphics or logos depicting companies/products shall not appear on publicly accessible DoD Web sites.

8.1.5. Organizations considering the use of "frames" technology to connect to external sites should consult legal counsel concerning trademark and copyright issues before establishing such links.

8.1.6. Organizations are encouraged to link to authorized activities in support of the organization's mission, such as the Army and Air Force Exchange Service (AAFES, http://www.aafes.com), the Navy Exchange Service Command (NEXCOM, http://www.navy-nex.com) and the Marine Corps Exchange. If these sites contain commercial advertisements or sponsorships, the appropriate disclaimer below shall be given.

8.1.7. When external links to non-government Web sites are included, the head of the DoD Component, or the subordinate organization, is responsible for ensuring that a disclaimer is made that neither the DoD nor the organization endorses the product or organization at the destination, nor does the DoD exercise any responsibility over the content at the destination. This includes credits given to contractors who produce DoD Web sites.

8.1.8. When a publicly accessible DoD Web site is intended to serve a public purpose, organizations must realize that once the decision is made to include a link to one non-DoD site, the organization may have to link to all similar sites.

8.2. Disclaimer for External Links. The disclaimer below shall be displayed when linking to external sites. This disclaimer may appear on the page or pages listing external links, or through an intermediate "exit notice" page generated by the server machine whenever a request is made for any site other than the official DoD Web site (usually the .mil domain). An example of such an exit notice is located at the White House WWW site at http://www.whitehouse.gov/.

> "The appearance of hyperlinks does not constitute endorsement by the (Department of Defense/the U.S. Army/the U.S. Navy/the U.S. Air Force /the U.S. Marine Corps, etc.) of this Web site or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation sites, the (Department of Defense/the U.S. Army/the U.S. Navy/the U.S. Air Force/the U.S. Marine Corps, etc.) does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD Web site."

8.3. DoD Newspapers. The policies and procedures in DoD Instruction 5120.4 (reference (n)) apply to all DoD newspapers and civilian enterprise publications, whether printed or electronic. DoD funded newspapers and editorial content of civilian enterprise publications may be posted on DoD Web sites without advertising. Commanders and heads of organizations are authorized to link to a commercial/civilian Web site carrying the authorized civilian enterprise publications, which include advertising, provided the standard disclaimer for external links is given.

9. IMAGE MANIPULATION STANDARDS

Official DoD imagery provided on publicly accessible DoD Web sites must conform to DoD Directive 5040.5 (reference (g)).

10. COMMERCIAL SPONSORSHIP AND ADVERTISING

Commercial sponsorships, advertisements and endorsements are prohibited on publicly accessible pages of official DoD Web sites. Publicly accessible Web sites are official communications to the public. Just as the DoD would not print advertisements on news releases, the Department shall not post advertisements on publicly accessible official DoD Web sites. Organizations shall ensure that the credibility of official information is not adversely affected by association with commercial sponsorships, advertisements or endorsements.

10.1. Non-appropriated Fund Activities and Web sites. In accordance with DoD Instruction 1015.10 (reference (m)). Morale, Welfare and Recreation (MWR) programs may have commercial sponsors and may sell electronic advertising as outlined in that instruction. As the instruction points out, MWR products with advertisements are intended for distribution to the DoD internal audience authorized to take advantage of these programs.

10.1.1. However, having advertisements on pages that are part of an official, publicly accessible DoD Web site is inappropriate. Organizations are encouraged to include official information about non-appropriated fund (NAF) activities on official DoD Web sites as long as the information does not include commercial sponsorships or advertisements.

10.1.2. With organization approval, NAF activities may use non-appropriated funds to develop and maintain commercial Web sites for unofficial information, where commercial sponsorship or advertising may appear. External links to authorized, unofficial NAF commercial Web sites are authorized, with an appropriate disclaimer preceding the actual connection to the NAF commercial Web site to avoid product endorsement or preferential treatment.

10.1.3. Official information pertaining to the NAF activity may be posted on the commercial non-appropriated fund Web site with installation commander/organization head approval, but only if it is also posted on the official publicly accessible DoD Web site. Other official information shall not be posted to the commercial site.

11. DESIGN STANDARDS AND NON-STANDARD FEATURES

11.1. Web site documents shall conform to the approved technical specifications approved in the Joint Technical Architecture (JTA). In situations where World Wide Web Consortium (W3C) recommendations or proposed recommendations are more recent than those examined by the JTA, developers may use the W3C recommendations or proposed recommendations.

11.2. Incorporation of non-standard or browser-specific features into Web pages shall also be evaluated in light of the potential security risks and interoperability. Certain features have the capability of installing malicious programs on networks or on individual machines, if downloaded. The same danger exists when downloading any executable file, which is why many organizations have a policy in place prohibiting downloads of such files. In general terms, it is

recommended that existing local guidelines concerning the download/installation of executable files should apply to any software that installs programs on networks or individual machines. Use of non-standard or browser specific features may exclude a portion of a Web site's audience, and should be avoided.

12. COLLECTION OF INFORMATION

In certain instances it is necessary and appropriate to collect information from visitors to Web sites. Agencies subject to DoD Directive 5240.1 (reference (q)) must comply with its provisions in addition to those cited below.

12.1. Compliance with the Paperwork Reduction Act. Publicly accessible Web sites shall comply with the requirements of Paperwork Reduction Act of 1995 (PRA), (reference (a)), as described below. The PRA requires that collection of information from the public be approved by OMB under some circumstances.

12.1.*1*. Requests for identical information from ten or more members of the public*, to include DoD contractors,* must be approved by OMB*. Such requests include* surveys using check box, radio button or text form fields.

12.1.*2*. The PRA applies to electronic forms/information collections on Web sites that collect standardized information from the public. It does not apply to collection of information strictly from current DoD employees or service members in the scope of their employment. Surveys on publicly accessible Web sites will not ordinarily be exempt from the requirement to obtain OMB approval under this exception.

12.1.*3*. Forms for general solicitations of comments that do not seek responses to standard questions, such as the common opinion-based feedback forms and e-mail links, do not require OMB clearance. *See, however, paragraph 12.2 below.*

12.1.*4*. Organizations are responsible for ensuring their publicly accessible Web sites comply with this requirement and follow procedures in DoD 8910.1-M (reference (l)). For more information about the Paperwork Reduction Act of 1995, contact your local Information Management Control Office.

12.2 Collection of Personally-identifying Information from DoD Web Sites. The solicitation or collection of personally identifying information, including automated collection or collection through capabilities which allow a user to contact the Web site owner or webmaster, triggers the requirement for either a Privacy Act Statement (PAS) or a privacy advisory (PA).

12.2.1 Use of a Privacy Act Statement.

12.2.1.1 Whenever personally-identifying information (see Part III, Definitions) is solicited from an individual (e.g., eligibility for benefits determinations) and the information is maintained in a Privacy Act system of records (i.e., information about the individual is retrieved by name or other personal identifier), a Privacy Act Statement (PAS), consistent with the requirements of reference (mm), must be posted to the Web page where the information is being solicited or provided through a well-marked hyperlink.

12.2.1.2 If the information collected is being maintained in a Privacy Act system of records for which a notice has not yet been published in the Federal Register, such a notice must be published, consistent with the requirements of the Act, prior to any information being collected.

12.2.1.3 If a PAS would be required if the solicitation were made in the paper-based world, it is required in the on-line world, whether the site is publicly accessible or non-publicly accessible.

12.2.2 Use of a Privacy Advisory.

12.2.2.1. If personally-identifying information (see Part III, Definitions) is solicited by a DoD Web site (e.g., collected as part of an email feedback/comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA). The PA informs the individual as to why the information is being solicited (e.g., so that the Department can provide the information that has been requested by the individual) and how such information will be used (e.g., it will be destroyed after the information the individual is seeking has been forwarded to him or her).

12.2.2.2. If personally-identifying information (see Part III, Definitions) is solicited by a DoD Web site (e.g., as part of electronic commerce transactions), a PA must be provided regardless of where the information is maintained.

12.2.2.3. The PA must be posted to the Web page where the information is being solicited or provided through a well-marked hyperlink. Providing a statement such as "Privacy Advisory: Please refer to the Privacy and Security Notice that describes why this information is being collected and how it will be used." linked to the applicable portion of the privacy and security notice required by paragraph 7 above is satisfactory.

12.2.3 Automated Collection of Information on Publicly Accessible Web Sites

12.2.3.1 Use of Session Cookies. The use of session cookies (see Part III, Definitions) is permitted for session control and to maintain state, but such cookies shall expire at the end of the logical session. Data from those cookies may not be utilized for other purposes or stored subsequently. The use of session cookies shall be explicitly identified in the site's privacy notice (see Part V, paragraph 4.1).

12.2.3.2 Use of Persistent Cookies. The use of persistent cookies is authorized only if all of the following conditions are met:
(a) there is a compelling need to gather the data on the Web site;
(b) appropriate technical procedures have been established to safeguard the data;
(c) the Secretary of Defense has personally approved use of the cookie prior to implementation of the data collection; and
(d) privacy notices clearly specify, in addition to other required information, that cookies are being used and describe the safeguards for handling the information collected from the cookies.

Requests for approval to use persistent cookies should be submitted at least 30 days prior to operational need date, through the appropriate chain of command, to the Office of the Assistant Secretary of Defense (C3I), for processing prior to submission to the Secretary of Defense for decision. The request shall describe the need and the safeguards to be used to protect the data, provide an explanation of why other technical approaches are inadequate, and include a copy of the privacy notice(s) proposed for use.

12.2.3.3. Other Automated Means of Collecting Personally-identifying Information. The use of any other automated means to collect personally-identifying information without the express permission of the user requires the same approvals as described in paragraph 12.2.3.2 above.

12.*3*. Usage Statistics. As a management function, evaluation of site usage data (log files) is a valuable way to evaluate the effectiveness of Web sites. However, collection of data from publicly accessible sites for undisclosed purposes is inappropriate. There are commercially available software packages that will summarize log file data into usable statistics for management purposes, such as the most/least requested documents, type of browser software used to access the Web site, etc. Use of this type of software is appropriate, as long as there is full disclosure as specified in the privacy and security notice, referenced *in Paragragh 7* above. Organizations shall establish a destruction disposition schedule for collected data.

13. DoD WEBMASTER LISTSERV

To share and coordinate information, an e-mail listserv has been established for all DoD "Webmasters." All personnel responsible for developing and/or maintaining a Web site are encouraged to join this listserv. Although an Army unit maintains it, the list is open to members in all services. Instructions are located at http://www.army.mil/Webmasters/faq/.

14. EFFECTIVE DATE: These procedures are effective 120 days from the date of this document.

WEB SITE ADMINISTRATION

Part III – Definitions

November 25, 1998

With Amendment April 26, 2001 incorporated in red italics

Cookie. A "cookie" is a small piece of information (token) sent by a Web server and stored on a user's system (hard drive) so it can later be read back from that system. Using cookies is a convenient technique for having the browser remember some specific information. Cookies may be categorized as "session" or "persistent" cookies. "Session" cookies are temporary cookies that are used to maintain context or "state" between otherwise stateless Web transactions (e.g., to maintain a "shopping basket" of goods selected during a single logical session at a site) and that must be deleted at the end of the web session in which they are created. "Persistent" cookies remain over time and can be used for a variety of purposes, including to track a user's access over time and across Web sites, or to establish user preferences.

DefenseLINK. The name of the official publicly accessible Web site for the Department of Defense (DoD). DefenseLINK provides the official single point of access to all DoD information on the World Wide Web, and establishes a means to ensure that the information is readily accessible, properly cleared and released, accurate, consistent, appropriate and timely.

DoD Originating Office (DOO). Is the entity that created or sponsored the work that generated the information or received/acquired the information on behalf of the DoD.

Home page. The index or introductory document for a Web site.

Internet. The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information.

Operations Security (OPSEC). OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to defense acquisitions, military operations, and other activities in order to: i) identify those actions that can be observed by adversary intelligence systems; and ii) determine what indicators might be obtained by hostile intelligence systems that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and iii) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation

Official DoD Web site. A DoD Web site that is developed and maintained with command sponsorship and approval, and for which the DoD Component, a subordinate organization or individual, exercises editorial control over content. The content of official DoD Web sites is of an official nature that may be endorsed as the official position of the DoD Component. Content may include official news releases, installation history, command position

papers, etc. Official DoD Web sites are prohibited from displaying sponsorships or commercial advertisements.

Personally-Identifying Information. *Information, including, but not limited to, name, e-mail or postal address, or telephone number, that can be used to identify an individual.*

Technical Information. Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment. (JCS Pub 1)

Unofficial DoD Web site. A DoD Web site that is developed and maintained with non-appropriated funds; and for which the DoD Component, or a subordinate organization, does not usually exercise editorial control over content. The content of unofficial DoD Web sites is not endorsed as the official position of the DoD Component. Content will not normally include official news releases, installation history, command position papers, etc. Unofficial DoD Web sites may include sponsorships and commercial advertisements, and may also advertise products for sale, in accordance with the mission of the organization. In most cases, unofficial DoD Web sites are developed and maintained by commercial or nonprofit organizations. Certain military-affiliated organizations may develop and maintain unofficial DoD Web sites. Such organizations include service exchanges and Morale, Welfare and Recreation activities that use non-appropriated funds.

World Wide Web or Web. The subset of the Internet capable of providing the public with user-friendly graphics-based multi-media access to information on the Internet. It is the most popular means for storing and linking Internet-based information in all multi-media formats. Navigation is accomplished through a set of linked documents that may reside on the same computer or on computers located almost anywhere else in the world.

Web site. A collection of information organized into a number of Web documents related to a common subject or set of subjects, including the "home page" and the linked subordinate information.

Web Server Environment. The physical computing resources, including servers, software, network, communications, security, and peripheral devices that provide the platform upon which Web sites are made available to users through internetworking.

WEB SITE ADMINISTRATION

Part IV – References

November 25, 1998

With Amendment April 26, 2001 incorporated in red italics

(a) 44 USC Chapter 35, "Paperwork Reduction Act", as amended

(b) Government Printing and Binding Regulations, Joint Committee on Printing, Congress, US, February 1990, No. 26

(c) National Archives and Records Administration General Schedule 20, August 1995

(d) Deputy Secretary of Defense Policy Memorandum, "Government Information Locator Service (GILS)," September 2, 1995

(e) Chairman, Joint Committee on Printing Memorandum granting waiver for Commercial Enterprise Newspapers, July 15, 1983

(f) Office of Management and Budget (OMB) Bulletin 95-01, "Establishment of Government Information Locator Service," December 7, 1994

(g) DoD Directive 5040.5, "Alteration of Official DoD Imagery," August 29, 1995

(h) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996

(i) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 22, 1997

(j) DoD 5400.7-R, "DoD Freedom of Information Program Regulation", September 1998

(k) DoD 5500.7-R, Joint Ethics Regulation (JER), August 30, 1993

(l) DoD Directive 8910.1-M, "DoD Procedures for Management of Information Requirements," *June 30, 1998, authorized by DoD Directive 8910.1, "Management and Control of Information Requirements,"* June 11, 1993

(m) DoD Instruction 1015.10, "Programs for Morale, Welfare, and Recreation (MWR)," November 3, 1995, w/ Ch 1, October 31, 1996

(n) DoD Instruction 5120.4, "DoD Newspapers and Civilian Enterprise Publications," June 16, 1997

(o) DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release," May 6, 1996

(p) AR 60-20/AFR 147-14, "Army and Air Force Exchange Service Operating Policies," 15 December 1992

(q) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988

(r) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987

(s) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984

(t) Public Law 100-235, "Computer Security Act of l987"

(u) DoD Directive 5200.5, "Communications Security (COMSEC)," April 21, 1990

(v) DoD Directive 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997

(w) DoD Directive 4640.6, "Communications Security (COMSEC) Telephone Monitoring and Recording, " June 26, 1981

(x) DoD Directive 5205.2, "DoD Operations Security Program," July 7, 1983

(y) DoD Instruction 3200.14, "Principles And Operational Parameters of the DoD Scientific and Technical Information Program," May 13, 1997, Enl 6

(z) International Traffic in Arms Regulation (ITAR), Department of State, May 1998

(aa) Wassenaar Arrangement, see Federal Register, January 15, 1998 (Vol 63 No. 10) pages 2451 – 2500

(bb) Carnegie Mellon University Software Engineering Institute, "Security for a Public Web Site," CMU/SEI-SIM-002, August 1997

(cc) National Institute of Standards and Technology (NIST), "Internet Security Policy: Technical Guide," http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

(dd) Defense Information Systems Agency (DISA), "DISA/NCS World Wide Web (WWW) Handbook Version 2.2," http://www.disa.mil/handbook/toc.html

(ee) DoD Directive 8500.xx, "Information Assurance," draft

(ff) DoD Instruction 8500.xx, "Information Assurance Requirements," draft

(gg) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," August 1997.

(hh) DoD General Counsel Memorandum, "Communication Security and Information Systems Monitoring," March 17, 1997

(ii) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

(jj) DoD 5025.1-M, "DoD Directive Systems Procedures, August 1994

(kk) DoD 5200.1-R, "Information Security Program, " January 1997

(ll) USD (P&R) and OASD (C3I) memorandum entitled "Information Assurance (IA) Training and Certification," June 29, 1998.

(mm) Section 552a of title 5, United States Code, as implemented by DoD 5400.11-R, "Department of Defense Privacy Program, " August 1983.

WEB SITE ADMINISTRATION

Part V – Examples & Best Practices

November 25, 1998

With Amendment April 26, 2001 incorporated in red italics

1. INFORMATION VULNERABILITY, THE WEB AND OPSEC

1.1. General

1.1.1. Over the last three decades, the world has experienced the rapid integration of information processes and telecommunications technology. As we leveraged these gains, the national security posture of the United States has become increasingly dependent on the Defense (DII), National (NII) and the larger Global Information Infrastructure (GII). These information infrastructures (which consist of information, information systems, telecommunications, networks, and technology) represent lucrative targets in an increasingly asymmetrical threat environment.

1.1.2. Within this global infrastructure lies a mosaic of interconnectivity which is growing at a rate of 500,000 new World Wide Web (WWW) entry points a month. This interconnectivity, when coupled with search engines and information compilation algorithms, provides a single user the ability to aggregate, analyze, and construct new levels of understanding from unclassified sources. As such, the information provided on publicly accessible Web sites is an OPSEC concern.

1.1.3. This section addresses why information technology makes sensitive but unclassified information vulnerable. It will address why certain types of DoD information cannot be posted to publicly accessible Web sites within the context of the OPSEC process.

1.2. Information Technology

1.2.1. The information infrastructure is extremely complex. There is no simple way to define and establish its bounds, to measure its impact, or to identify clear responsibilities for its evolution, operation, maintenance, and repair. Therefore, the various views of the infrastructure presented here only partially address the complexity.

1.2.2. One way of viewing the information infrastructure is in terms of its basic components. In simple terms, the information infrastructure is comprised of the components necessary for the transportation of information, the information itself, the means for creating, gathering, and processing data to obtain information, and the storage of the data and information.

1.2.3. Another way of viewing the information infrastructure is as a collection of networks and services. Some of these networks and services, such as the Internet and public telephone and data networks, have an identity of their own and are clearly an integral part of the Information infrastructure. Others, such as financial networks and services, have developed within a specific industry and evolved into a complex inter-network necessary to provide responsive support to the customer. This is particularly true regarding the Defense Information Infrastructure (DII).

1.2.4. The information infrastructure can also be thought of in terms of the various domains it serves. These infrastructure domains have the potential of containing vast amounts of sensitive but unclassified information. This has not gone unnoticed by Internet users who have developed and are now refining sophisticated “data mining” tools and techniques that allow precision targeting and rapid aggregation of data.

1.2.5. When you combine these infrastructure components, networks and services, and domains, the OPSEC oriented user will quickly recognize the vast resources of information available to the public and the adversary. The potential for inadvertent or unauthorized disclosure of sensitive information continues to grow.

1.3. Information Vulnerability and the OPSEC Process

1.3.1. Given the increasing dependence of our national and economic security upon the information infrastructure, it is essential that the commander and other organizational Heads review organizational information connectivity and content to ensure good OPSEC procedures are being applied within their organizations. As such, risk assessment and risk management become critical factors in evaluating publicly accessible Web site information.

1.3.2. The worldwide connection of computer local area networks (LAN) and wide area networks (WAN) such as the NIPRNET makes access to defense information from anywhere in the world relatively easy. Separation between the NIPRNET and the WWW is ambiguous, and occasionally these networks may be indistinguishable to Web page administrators. Web pages intended for internal DoD use should not be made available on the NIPRNET without appropriate access control, as this information is likely to be accessible to non-DoD users. Consequently, OPSEC and INFOSEC concerns arise.

1.3.3. This requires a convergence of Information Security (COMPUSEC and COMSEC) tools and the OPSEC process at the activity level. Activity webmasters, page maintainers, subject matter experts and OPSEC personnel must develop a disciplined review of all information posted to their locally generated Web sites. This must be done to protect sensitive unclassified and classified information -- while recognizing the importance of making available timely and accurate information to the intended DoD audiences, the public, Congress, and the news media.

1.3.4. Evaluations of activity information provided on the NIPRNET and publicly accessible DoD Web sites on the Internet should follow current OPSEC methodology:

1.3.4.1. Identify information access points (NIPRNET, Internet, etc.,..) and evaluate their importance to activity operations.

1.3.4.2. Determine the critical information for the activity's operations and plans. Information that would not be of interest/use to the general public should not be on a public access page.

1.3.4.3. Determine the threat –assume that any potential adversary has access and knows how to search the net.

1.3.4.5. Determine the vulnerabilities – how protected are the Web pages? Remember, the hacker is generally the INFOSEC threat, the search engine and browser are generally the OPSEC threat.

1.3.4.6. Assess the risk – what protection should be applied to minimize potential loss of critical information and what is the impact on operations and operations support?

1.3.4.7. Apply protection – combine INFOSEC and OPSEC tools to minimize information loss and vulnerability.

1.3.5. When applying the OPSEC process to information posted to Web sites, the activity will also need to evaluate subject data with regard to the time factor. Information gathering in the past was a manpower and resource intensive process that was dependent on various types of overt and clandestine means. Collection, compilation, analysis, and dissemination of information could take days, weeks, or months. Today, a single user can connect to the Web and using varying search engines, browsers, and certain aggregation methods develop a composite of information that surpasses traditional knowledge levels. In essence, geography is no longer a factor in information retrieval--time becomes the dominant factor.

1.3.6. As such, the user must determine the value of information with regards to time. Certain data such as unit history, emblems, command affiliation, etc. will have less time criticality than will deployment orders for exercises or real world operations. The value of information may also flex over time. For example, the specifics of post-deployment preparations should not be posted to a publicly accessible Web site prior to the deployment. But once in theater, unit types, number of personnel and equipment will become public knowledge over time, decreasing the sensitivity of the data. Subsequently, the same information will again become sensitive as redeployment dates and unit withdrawal specifics are planned. This will require units to actively scrub their Web pages for time sensitive data.

1.4. Conclusion. Operations security is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other sensitive activities. OPSEC training and education apply to computer use just as it does in conversations between personnel, correspondence, and telephone conversations. In the past, OPSEC has focused on activities that might be seen by a human observer, a satellite, a radio intercept operator or the news. But with the proliferation of information technologies over the last three decades, the access to DoD data has grown exponentially. The old threats have not gone away, but there is a new area of concern that OPSEC officers and planners must consider – the Internet. A disciplined approach to INFOSEC procedures in conjunction with the OPSEC process will ensure that sensitive but unclassified information is properly safeguarded.

2. GUIDE FOR IDENTIFYING INFORMATION INAPPROPRIATE FOR POSTING TO A PUBLICLY ACCESSIBLE DOD WEB SITE

This guidance is authorized to be used for one purpose only: identifying information that may be inappropriate for posting to publicly accessible DoD Web sites. **It is not to be used as guidance in responding to requests under the FOIA or the Privacy Act under any circumstances.** It is intended as an interim guide to the identification of categories of information that are inappropriate for posting to a publicly accessible Web site. Additional guidance will be forthcoming when this document is formalized in the DoD publication system.

FOR OFFICIAL USE ONLY (FOUO) information may not be posed to official Web sites that are open to public access. (Information which is typically FOUO is followed by an * below). Also identified below is information whose sensitivity may be increased when electronically aggregated in significant volume. All information proposed for posting to a publicly accessible Web site must be reviewed in accordance with the provisions of DoD Directive 5230.9 and DoD Instruction 5230.29 (references (h) and (o)) and as described in Paragraph 3, Part II of this document.

Do not use this compendium as the sole source for identifying such information. Questions about FOUO information should be referred to your local FOIA office. Questions about aggregated information should be referred to your local security office and/or OPSEC coordinator.

2.1 Military Operations & Exercises information relating to:

- Unit Organization
- Unit readiness specificity
- Detailed mission statement
- Specific Unit phone/fax numbers (secure and unsecured)
- Time-Phase Force Deployment Data (TPFDD)
- Ops schedules
- Logistics support requirements
    - Medical
    - Civil engineering
    - POL
    - Host nation support
    - Transportation
    - Munitions
- Force Apportionment
- Force Allocation
- Unit Beddown information
- Planning guidance
- Unit augmentation
- Force Synchronization
    - Unit shortfalls
- Counter-terrorism information
- Detailed Budget Reports
- Images of Command and Control (C2) nodes
- Inventory reports
- Intelligence, Surveillance and Reconnaissance (ISR) Capabilities
- Command, Control, Communications, Computers and Intelligence(C4I) Architecture
- Non-Combatant Evacuation Operations (NEO) Plans or Ops
- Counter-drugs Ops
- Unit Recall Rosters
- Weapons Movements
- Mobilization information
- Detailed maps or installation photography
- Standard Operating Procedures
- Tactics, Techniques, and Procedures
- Critical maintenance

2.2. Personnel information relating to:

- Information, the release of which would be a clearly unwarranted invasion of personal privacy, to include the following categories about U.S. citizens, DoD employees and military personnel: (1) Social Security Account Numbers; 2) dates of birth; 3) home addresses, and 4) telephone numbers other than duty office

numbers. Duty phone numbers of units described in C.3.2.1.6.2.2. of DoD 5400.7-R (reference (j)) may not be posted.*

- Names, locations, and any other identifying information about family members of DoD employees and military personnel*
- Official travel itineraries of individuals and units before it is performed*
- Duty rosters, or detailed organizational charts and directories with names (as opposed to organizational charts, directories, general telephone numbers for commonly requested resources, services and contacts without names)*
- Internal DoD personnel rules and practices unless cleared for release to the public*
- Financial Disclosure Reports of Special Government Employees (5 USC App. 4, §207 (a) (1) 2)*
- Representation Rights and Duties, Labor Unions (5 USC §7114 (b)(4))*
- Action on reports of Selection Boards (10 USC §618)*
- Confidential Medical Records (10 USC §1102)*
- Civil Service Examination (18 USC §1917)*
- Drug Abuse Prevention/Rehabilitation Records (21 USC §1175)*
- Confidential of Patient Records (42 USC §290dd-2)*
- Information Concerning US Personnel Classified as POW/MIA During Vietnam Conflict (42 USC §401)*
- Information Identifying Employees of DIA, NRO, and NIMA (10 USC §424)*

2.3. Proprietary Information submitted by a contractor and protected by a Limited Rights Statement or other agreement, and trade secrets, commercial and financial information submitted by an entity outside the government that considers the information to be protected from release to the public. Other specific provisions include:

- Contractor Proposals (10 USC §2305 (g))*
- Commercial or financial information received in confidence with loans, bids, contracts or proposals*
- Information received in confidence e.g. trade secrets, inventions, discoveries or other proprietary data*
- Statistical data and commercial or financial information concerning contract performance, income, profits, losses and expenditures, if offered and received in confidence from a contractor or potential contractor*
- Scientific and manufacturing processes or developments concerning technical or scientific data and other information submitted with an application for research grant or with a report while research is in progress*
- Test and evaluation of commercial products or military hardware produced by a non-governmental entity*
- Patents, unless licensed for publication by the United States*
- Software documentation: shall be distributed according to the terms of the software license*

- Premature Dissemination: The information related to patentable military systems or processes in the developmental stage.*
    - Confidential Status of Patent Applications (35 USC §122)*
    - Secrecy of Certain Inventions and Withholding of Patents (35 USC §181-188)*
    - Confidential Inventions Information (35 USC §205)*

2.4. Test and Evaluation information could result in an unfair advantage or disadvantage to the manufacturer or producer or could reveal the capabilities, limitations, or incapabilities of a DoD weapons systems or component.

2.5. Scientific and technological information relating to:

- Critical technology on either the Munitions List or the Commerce Control List*
- Unclassified Special Nuclear Weapons Information (10 USC §128)*
- Unclassified Technical Data with Military or Space Application (10 USC §130)*
- Centers for Industrial Technology – Reports of Technology Innovations (15 USC §3705 (e)(E))*
- Information Regarding Atomic Energy (42 USC §2161-2168)*
- Control of Arms Exports Sec 38(e) of the Arms Export Control Act (22 USC §2778(e))*
- Technical and scientific data developed by a contractor or sub-contractor exclusively or in part at private expense*
- Sensitive S&T Reports such as:*
    - Defense Acquisition Executive System Reports
    - Selected Acquisition Reports
    - Weapons System Unit Cost Reports
    - Approved Program Baselines for ACAT I, II, III Weapons Systems
    - Weapons Systems Evaluation and Testing Results and Reports
    - Reports Based on Joint USA and Foreign Government Technical Research and Weapons Systems Evaluations
    - Weapons System Contractor Performance Reporting Under earned Value Reporting System at the Level of CPE Reporting
    - Weapons Systems staff working papers, correspondence and staff assessments
    - DoD Component “Feedback” staff working papers and assessments on weapons System Program Performance

2.6. Intelligence information relating to:

- Organizational & Personnel Information for DIA, NRO and NIMA (10 USC §424)*

- Maps, Charts, and Geodetic Data (10 USC §455)*
- Communications Intelligence (18 USC §798)*
- NSA Functions and Information (50 USC §402)*
- Protection of Identities of US Undercover Intelligence Officers, Agents, Informants and Sources (50 USC §421)*
- Protection of Intelligence Sources and Methods 50 USC §403(d)(3))*

2.7. Other information relating to:

- A-76 studies and other outsourcing studies that provide detailed descriptions of sensitive organizational operations
- Administrative Dispute Resolutions (5 USC §574 (j))*
- Confidentiality of Financial records (12 USC §3403)*
- National Historic Preservation (16 USC §470w-3)*
- Internal advice, recommendations and subjective evaluations*

3. SECURITY AND ACCESS CONTROLS

3.1. Determinations as to the appropriate security and access controls to employ will be based upon the sensitivity of the information and the target audience for which it is intended. The table below provides additional guidance to include the vulnerability of various combinations of each. Use this table in conjunction with the above list of types of sensitive information to determine an acceptable level of risk. Do not regard these guidelines as the only options available for protecting information content.

If access control is:	and transmission control is:	the vulnerability is:	and the information posted can be:
Open – Includes Webmaster training and certification, isolation of the server, current version of server software and O/S, with all security patches properly installed	Plain text, unencrypted	Extremely High – Subject to worldwide dissemination and access by everyone on Internet	Non-sensitive, of general interest to the public, cleared and authorized for public release for which worldwide dissemination poses limited risk for DoD or DoD personnel, even if aggregated with other information reasonably expected to be in public domain.
Limited by Internet Domain (e.g. .mil, .gov) or IP address	Plain text, unencrypted	Very High – Can circumvent access controls, affords lowest level of access control, and no encryption	Non-sensitive, not of general interest to the public although approved and authorized for public release, and intended for DoD or other specifically targeted audience.
Limited By User ID and password (e.g. DMDC database or other registration system)	Plain text, unencrypted	High – Can circumvent access controls, affords higher level of access controls, however, IDs and passwords can be compromised if encryption is not used.	Non-sensitive but limited to a specific, targeted audience.
User Certificate Based (Software) Requires PKI	Encrypted text through use of secure sockets layer	Moderate – Provides moderate level of access controls	FOR OFFICIAL USE ONLY and information sensitive by aggregation
User Certificate Based (Hardware) Requires PKI	Encrypted text	Very Low	FOR OFFICIAL USE ONLY and information sensitive by aggregation where extra security is required due to compilation

Table 1. Security and Access Controls

3.2. Until such time as specific technical policy guidelines are formalized for all Internet services, Webmasters and users are encouraged to consult existing authoritative literature on security and access controls. Examples of such literature include, but are not limited to:

3.2.1. Carnegie Mellon University Software Engineering Institute, “Security for a Public Web Site,” CMU/SEI-SIM-002, August 1997.

3.2.2. National Institute of Standards and Technology (NIST), “Internet Security Policy: A Technical Guide,” http://csrc.nist.gov/isptg/html/ISPTG-Contents.html

3.2.3. Defense Information Systems Agency (DISA), “DISA/NCS World Wide Web (WWW) Handbook Version 2.2,” “http://www.disa.mil/handbook/toc.html”

4. TEXT OF PRIVACY AND SECURITY NOTICE

4.1. The following privacy and security notice may be tailored in the indicated areas by each organization sponsoring a publicly accessible Web site. The notice shall be approved by the appropriate local legal authority before use.

Link from Index.html pages -- “Please read this privacy and security notice.”

( ) - indicates sections to be tailored at the installation level

[ ] - indicates hyperlinks

* - indicates information located at the hyperlink destination indicated

Quote:

PRIVACY AND SECURITY NOTICE

1. (DefenseLINK) is provided as a public service by the ([Office of the Assistant Secretary of Defense-Public Affairs] and the [Defense Technical Information Center]).

2. Information presented on (DefenseLINK) is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. For site management, [information is collected]* for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with [National Archives and Records Administration Guidelines].

Agencies subject to DoD Directive 5240.1 shall add the following to paragraph 5: "All data collection activities are in strict accordance with DoD Directive 5240.1 (reference (p))."

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward them to (us using the DefenseLINK [Comment Form].

The following, when appropriately tailored, may be used as a notice for sites using session cookies.

8. Cookie Disclaimer. (DefenseLINK) does not use persistent cookies, i.e., tokens that pass information back and forth from your machine to the server and remain after you close your browser. (DefenseLINK) does use session cookies, i.e., tokens that remain active only until you close your browser, in order to (make the site easier for you to use). No database of information obtained from these cookies is kept and when you close your browser, the cookie is deleted from your computer. (DefenseLINK) uses cookies in the following ways:

· (Describe use, e.g., "to save you time in filling out forms," "to maintain a relationship between the image and the correct link, the program that displays the banners on the bottom of some of our pages uses a session cookie.")

You can chose not to accept these cookies and still use the site, but (you may need to enter the same information repeatedly and clicking on the banners will not take you to the correct page). The help information in your browser software should provide you with instruction on how to disable cookies.

_____ ***End Quote***:

* Link from above - "information is collected" to the following text:

NOTE: The information below should be tailored, if necessary, to show an accurate example of the specific information being collected.

Example: Information Collected from (DefenseLINK) for Statistical Purposes

Below is an example of the information collected based on a standard request for a World Wide Web document:

> xxx.yyy.com - - [28/Jan/1997:00:00:01 -0500] "GET /DefenseLINK/news/nr012797.html HTTP/1.0" 200 16704 Mozilla 3.0/www.altavista.digital.com

xxx.yyy.com (or 123.123.23.12)-- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (.com) the requester is coming from a commercial address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[28/Jan/1997:00:00:01 -0500] -- this is the date and time of the request

"GET /DefenseLINK/news/nr012797.html HTTP/1.0" -- this is the location of the requested file on (DefenseLINK)

200 -- this is the status code - 200 is OK - the request was filled

16704 -- this is the size of the requested file in bytes

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages

www.altavista.digital.com - this indicates the last site the person visited, which indicates how people find (DefenseLINK)

Requests for other types of documents use similar information. *No personally-identifying information is collected.*

4.2. The following notice and consent banner, approved by the DoD General Counsel (reference (hh)), may be used on all DoD Web sites with security and access controls. This banner may be tailored by an organization but such modifications shall be accomplished in compliance with reference (hh), and shall be approved by the Component's General Counsel before use.

> "This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system,

to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes."